p-REGULARITY OF THE p-ADIC VALUATION OF THE FIBONACCI SEQUENCE

LUIS A. MEDINA AND ERIC S. ROWLAND

Abstract. This paper studies the p-adic valuation of the sequence $\{F_n\}_{n\geq 1}$ of Fibonacci numbers from the perspective of regular sequences. We establish that this sequence is p-regular for every prime p and give an upper bound on the rank for primes such that Wall's question has a negative answer. We also point out that for primes $p \equiv 1, 4 \mod 5$ the p-adic valuation of F_n depends only on the p-adic valuation of n and on the sum modulo $p-1$ of the base-p digits of n — not the digits themselves or their order.

1. Introduction

Consider integers $k \geq 2$ and $n \geq 1$. The exponent of the highest power of k that divides n is denoted by $\nu_k(n)$. For example, $\nu_2(144) = 4$. If $k = p$ is prime, $\nu_p(n)$ is called the *p-adic valuation* of n. Note the unsurprising fact that $\nu_k(n)$ depends only on the number of trailing zeros in the base-k representation of n; we will see momentarily a similar property in Fibonacci numbers for certain primes.

Let F_n be the nth Fibonacci number. Let $a \bmod k$ denote the least nonnegative integer b such that $a \equiv b \mod k$. For a fixed $k \geq 1$, the sequence $F_n \bmod k$ is periodic; we denote the "Pisano" period length of this sequence by $\pi(k)$. Let $\alpha(k)$ be the smallest value of $n \geq 1$ such that $k \mid F_n$; this is often called the *restricted period length* modulo k. It is well known that $\alpha(k)$ divides $\pi(k)$ [8, Theorem 3]. Throughout the paper we will also use the following classical result [6, 3], where $\left(\frac{a}{b}\right)$ is the Legendre symbol.

Theorem 1.1. *Let p be a prime. Then $\alpha(p) \mid p - \left(\frac{5}{p}\right)$. Furthermore, if $p \equiv 1, 4 \mod 5$ then $\pi(p) \mid p-1$, and if $p \equiv 2, 3 \mod 5$ then $\pi(p) \mid 2(p+1)$.*

Lengyel [4] discovered the structure of $\nu_p(F_n)$ for prime p.

Theorem 1.2 (Lengyel)**.** *For $n \geq 1$,*

$$\nu_2(F_n) = \begin{cases} \nu_2(n)+2 & \text{if } n \equiv 0 \mod 6 \\ 1 & \text{if } n \equiv 3 \mod 6 \\ 0 & \text{if } n \equiv 1,2,4,5 \mod 6, \end{cases} \tag{1.1}$$

$\nu_5(F_n) = \nu_5(n)$, and for a prime $p \neq 2, 5$

$$\nu_p(F_n) = \begin{cases} \nu_p(n) + \nu_p(F_{\alpha(p)}) & \text{if } \alpha(p) \mid n \\ 0 & \text{if } \alpha(p) \nmid n. \end{cases} \tag{1.2}$$

Date: October 12, 2009.
2000 *Mathematics Subject Classification.* Primary 11, Secondary 68.
Key words and phrases. valuations, Fibonacci numbers, k-regular sequence.

Remark. It is known that $\nu_p(F_{\alpha(p)}) = 1$ for every prime $p < 2 \times 10^{14}$ [5]. The statement $\nu_p(F_{\alpha(p)}) = 1$ is equivalent to $\pi(p^2) \neq \pi(p)$, and the question whether there is some prime for which this does not hold is known as Wall's question [8], which remains unresolved. We include it as a hypothesis (for primes $p > 2 \times 10^{14}$) in the first several theorems of the next section.

Our first theorem shows that for primes $p \equiv 1, 4 \mod 5$ the property of being able to change digits in the base-p representation of n in certain ways without affecting the p-adic valuation is carried over to $\nu_p(F_n)$ from $\nu_p(n)$. Let $s_k(n)$ denote the sum of the base-k digits of n.

Theorem 1.3. *Let $p \equiv 1, 4 \mod 5$ be a prime. Then $\nu_p(F_n)$ depends only on $s_p(n) \bmod \alpha(p)$ and on the length of the trailing block of zeros in the base-p representation of n.*

Proof. By Theorem 1.1, $p \equiv 1 \mod \alpha(p)$. Therefore $n \equiv s_p(n) \mod \alpha(p)$, so n is divisible by $\alpha(p)$ precisely when $s_p(n)$ is divisible by $\alpha(p)$, and the statement then follows from Theorem 1.2. □

Example 1.4. Any two integers with the same number of trailing zeros and the same digit sum modulo $p-1$ have corresponding Fibonacci numbers with the same exponent of p. For example, let $p = 11$. Writing numbers in base 11 with a representing the digit 10, $\nu_p(F_{16805000}) = 4 = \nu_p(F_{a000})$. In base 10, this reads $\nu_{11}(F_{31411600}) = \nu_{11}(F_{13310})$.

Example 1.5. If there are no zeros in the base-p representation of n, then permuting the digits does not affect the p-adic valuation of the corresponding Fibonacci number. Again writing numbers in base $p = 11$, we have $\nu_p(F_{1289}) = \nu_p(F_{1298}) = \nu_p(F_{1829}) = \cdots = \nu_p(F_{9821}) = 1$. In base 10, $\nu_{11}(F_{1670}) = \nu_{11}(F_{1680}) = \nu_{11}(F_{2330}) = \cdots = \nu_{11}(F_{12970}) = 1$.

2. p-REGULARITY

In this section we show that for every prime p the sequence $\{\nu_p(F_{n+1})\}_{n\geq 0}$ belongs to the class of p-regular sequences introduced by Allouche and Shallit [1]. First we recall the definition of a k-regular sequence.

For $k \geq 2$, the *k-kernel* of a sequence $\{a(n)\}_{n\geq 0}$ is the set of subsequences

$$\{\{a(k^e n + i)\}_{n\geq 0} : e \geq 0, 0 \leq i \leq k^e - 1\}. \tag{2.1}$$

A sequence is *k-regular* if the $\mathbb{Z}$-module generated by its k-kernel is finitely generated. For example, the sequence $\{\nu_k(n+1)\}_{n\geq 0}$ is k-regular: The $\mathbb{Z}$-module is generated by $\{\nu_k(n+1)\}_{n\geq 0}$ and $\{\nu_k(k(n+1))\}_{n\geq 0}$, since we can write each of the subsequences $\{\nu_k(kn+i+1)\}_{n\geq 0}$ and $\{\nu_k(k(kn+i+1))\}_{n\geq 0}$ for $0 \leq i \leq k-1$ as linear combinations of the two supposed generators as

$$\nu_k(kn+i+1) = \begin{cases} 0 & \text{if } 0 \leq i \leq k-2 \\ \nu_k(k(n+1)) & \text{if } i = k-1, \end{cases} \tag{2.2}$$

$$\nu_k(k(kn+i+1)) = \begin{cases} -\nu_k(n+1) + \nu_k(k(n+1)) & \text{if } 0 \leq i \leq k-2 \\ -\nu_k(n+1) + 2\nu_k(k(n+1)) & \text{if } i = k-1. \end{cases} \tag{2.3}$$

The *rank* of a k-regular sequence is the rank of the $\mathbb{Z}$-module generated by its k-kernel. Thus the rank of $\{\nu_k(n+1)\}_{n\geq 0}$ is 2.

Regular sequences have several nice characterizations, including the following "matrix ansatz" characterization [1, Lemma 4.1]. Let $n = n_l \cdots n_1 n_0$ be the standard base-k representation of n. The sequence $\{a(n)\}_{n\geq 0}$ is k-regular if and only if there exist $r \times r$ integer matrices $M_0, M_1, \ldots, M_{k-1}$ and integer vectors λ, κ such that

$$a(n) = \lambda M_{n_0} M_{n_1} \cdots M_{n_l} \kappa \tag{2.4}$$

for each $n \geq 0$. The matrix M_i contains the coefficients of the linear combinations of the generators that equal the ith subsequences of the generators. Thus r is the rank of the sequence. For example, the matrices for the choice of generators made above for $\{\nu_k(n+1)\}_{n\geq 0}$ are

$$M_0 = M_1 = \cdots = M_{k-2} = \begin{pmatrix} 0 & 0 \\ -1 & 1 \end{pmatrix} \text{ and } M_{k-1} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}. \tag{2.5}$$

The vector λ contains the coefficients of the linear combination of generators that equals $\{a(n)\}_{n\geq 0}$; since our first generator is the sequence $\{\nu_k(n+1)\}_{n\geq 0}$ itself, we take $\lambda = (1, 0)$. The vector $\kappa = (\nu_k(1), \nu_k(k)) = (0, 1)$ records the first term of each generator. We remark that $M_0 = M_1 = \cdots = M_{k-2}$ in this case reflects the fact mentioned at the beginning of the paper that $\nu_k(n)$ depends only on the number of trailing zeros in the base-k representation of n, and therefore $\nu_k(n+1)$ depends only on the positions of the digit $k-1$.

It does not obviously follow from Theorem 1.2 and the p-regularity of $\{\nu_p(n+1)\}_{n\geq 0}$ that the sequence $\{\nu_p(F_{n+1})\}_{n\geq 0}$ is p-regular. However, we give explicit generators and relations for the $\mathbb{Z}$-module generated by the p-kernel, establishing p-regularity and putting an upper bound on the rank of the sequence. The proofs (once one has guessed the relations) follow fairly mechanically from Theorem 1.2.

For $p = 2$, the sequences $\{\nu_2(F_{n+1})\}_{n\geq 0}$, $\{\nu_2(F_{2n+1})\}_{n\geq 0}$, $\{\nu_2(F_{(2n+1)+1})\}_{n\geq 0}$, $\{\nu_2(F_{4n+1})\}_{n\geq 0}$, and $\{\nu_2(F_{(4n+2)+1})\}_{n\geq 0}$ generate the $\mathbb{Z}$-module generated by the 2-kernel. One checks that they are linearly independent (for example, by looking at the first 16 terms of each), so $\{\nu_2(F_{n+1})\}_{n\geq 0}$ has rank 5. The matrices are

$$M_0 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad M_1 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

and encode the relations

$$\begin{aligned}
\nu_2(F_{(2n+0)+1}) &= \nu_2(F_{2n+1}) & \nu_2(F_{(2n+1)+1}) &= \nu_2(F_{(2n+1)+1}) \\
\nu_2(F_{2(2n+0)+1}) &= \nu_2(F_{4n+1}) & \nu_2(F_{2(2n+1)+1}) &= \nu_2(F_{(4n+2)+1}) \\
\nu_2(F_{(2(2n+0)+1)+1}) &= 3\nu_2(F_{2n+1}) & \nu_2(F_{(2(2n+1)+1)+1}) &= \nu_2(F_{4n+1}) + \nu_2(F_{(2n+1)+1}) \\
\nu_2(F_{4(2n+0)+1}) &= \nu_2(F_{2n+1}) & \nu_2(F_{4(2n+1)+1}) &= \nu_2(F_{4n+1}) \\
\nu_2(F_{(4(2n+0)+2)+1}) &= \nu_2(F_{(4n+2)+1}) & \nu_2(F_{(4(2n+1)+2)+1}) &= \nu_2(F_{2n+1}).
\end{aligned}$$

The first few of these are trivial, and the rest follow from applications of Theorem 1.2.

For $p = 5$, 5-regularity follows immediately from the 5-regularity of $\{\nu_5(n+1)\}_{n\geq 0}$. The rank is 2.

To make use of Theorem 1.1, we break the remainder of the primes into equivalence classes modulo 20. First we establish that $\{\nu_p(F_n)\}_{n\geq 0}$ is p-regular under the condition that Wall's question has an negative answer — that $\nu_p(F_{\alpha(p)}) = 1$ — and at the end we remove this condition. We start with the case $p \equiv 1, 4 \mod 5$. Consider the $p \times p$ matrices

$$M_0 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \; M_1 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 \\ 0 & 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 \\ 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \ldots, M_{p-2} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 & 0 & 1 \\ 0 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Finally, consider the $p \times p$ matrix

$$M_{p-1} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

and vectors

$$\begin{aligned} \lambda &= (1, 0, 0, \ldots, 0), \\ \kappa &= (\nu_p(F_1), \nu_p(F_1), \nu_p(F_2), \ldots, \nu_p(F_{p-1})). \end{aligned}$$

Theorem 2.1. *Let $p \equiv 1, 4 \mod 5$ be a prime such that $\nu_p(F_{\alpha(p)}) = 1$, and let $n \geq 0$. Then $\nu_p(F_{n+1}) = \lambda M_{n_0} M_{n_1} \cdots M_{n_l} \kappa$. In particular, $\{\nu_p(F_{n+1})\}_{n\geq 0}$ is a p-regular sequence of rank at most p.*

Proof. We will show that the p sequences $\{\nu_p(F_{n+1})\}_{n\geq 0}$ and $\{\nu_p(F_{pn+j+1})\}_{n\geq 0}$ for $0 \leq j \leq p-2$ generate the $\mathbb{Z}$-module generated by the p-kernel of $\{\nu_p(F_{n+1})\}_{n\geq 0}$. In particular, we show for $n \geq 0$ that

$$\nu_p(F_{(pn+i)+1}) = \begin{cases} \nu_p(F_{pn+i+1}) & \text{if } 0 \leq i \leq p-2 \\ \nu_p(F_{n+1}) + \nu_p(F_{pn+1}) & \text{if } i = p-1 \end{cases} \tag{2.6}$$

and that

$$\nu_p(F_{p(pn+i)+j+1}) = \nu_p(F_{pn+(i+j \bmod (p-1))+1}) \tag{2.7}$$

for $0 \leq i \leq p-1$ and $0 \leq j \leq p-2$. These are the relations encoded by the matrices M_i, so the theorem will then follow.

For both equations we will use the fact that since $p \equiv 1, 4 \mod 5$ then $\alpha(p)$ divides $p-1$ by Theorem 1.1.

Equation 2.6 is trivial for $0 \le i \le p-2$. To establish the case $i = p-1$ we use Theorem 1.2 to obtain

$$\nu_p(F_{pn+p}) = \begin{cases} \nu_p(n+1) + 1 + \nu_p(F_{\alpha(p)}) & \text{if } \alpha(p) \mid n+1 \\ 0 & \text{if } \alpha(p) \nmid n+1, \end{cases} \tag{2.8}$$

where we have used $\alpha(p) \nmid p$ since $\alpha(p) \mid p-1$ and $\alpha(p) > 1$. We also rewrite both terms in $\nu_p(F_{n+1}) + \nu_p(F_{pn+1})$ according to Theorem 1.2, noting that $\alpha(p) \mid n+1$ if and only if $\alpha(p) \mid pn+1$, since $n+1$ and $pn+1$ are congruent modulo $p-1$ and hence modulo $\alpha(p)$. Therefore

$$\nu_p(F_{n+1}) + \nu_p(F_{pn+1}) = \begin{cases} \nu_p(n+1) + 2\,\nu_p(F_{\alpha(p)}) & \text{if } \alpha(p) \mid n+1 \\ 0 & \text{if } \alpha(p) \nmid n+1. \end{cases} \tag{2.9}$$

The assumption $\nu_p(F_{\alpha(p)}) = 1$ implies $\nu_p(F_{(pn+p-1)+1}) = \nu_p(F_{n+1}) + \nu_p(F_{pn+1})$.

To establish Equation 2.7, we again use Theorem 1.2 to rewrite both sides. Since $1 \le j+1 \le p-1$, we have $\nu_p(p(pn+i)+j+1) = 0$, so

$$\nu_p(F_{p(pn+i)+j+1}) = \begin{cases} \nu_p(F_{\alpha(p)}) & \text{if } \alpha(p) \mid p(pn+i)+j+1 \\ 0 & \text{if } \alpha(p) \nmid p(pn+i)+j+1. \end{cases} \tag{2.10}$$

Since $1 \le (i+j \bmod (p-1))+1 \le p-1$, we have $\nu_p(pn+(i+j \bmod (p-1))+1) = 0$, so

$$\nu_p(F_{pn+(i+j \bmod (p-1))+1}) = \begin{cases} \nu_p(F_{\alpha(p)}) & \text{if } \alpha(p) \mid pn+(i+j \bmod (p-1))+1 \\ 0 & \text{if } \alpha(p) \nmid pn+(i+j \bmod (p-1))+1. \end{cases} \tag{2.11}$$

Again the two cases on either side of the equation coincide, since $p(pn+i)+j+1$ and $pn+(i+j \bmod (p-1))+1$ are congruent modulo $p-1$ and hence modulo $\alpha(p)$, so $\nu_p(F_{p(pn+i)+j+1}) = \nu_p(F_{pn+(i+j \bmod (p-1))+1})$ and the proof is complete. □

Let $\mathcal{M}_{p-1} = \{M_0, M_1, \ldots, M_{p-2}\}$. Note that the elements of $\mathcal{M}_{p-1}$ satisfy $M_i \cdot M_j = M_{i+j \bmod (p-1)}$, so $\mathcal{M}_{p-1}$ is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z}$ as a group. Therefore, each subproduct in $\nu_p(F_{n+1}) = \lambda M_{n_0} M_{n_1} \cdots M_{n_l} \kappa$ consisting of matrices from $\mathcal{M}_{p-1}$ depends only on the sum of the indices modulo $p-1$, which is a weakened version of Theorem 1.3. Note that the matrix M_{p-1} does not commute with any of the matrices in $\mathcal{M}_{p-1}$, which of course is necessary because $\nu_p(F_{n+1})$ depends on the number of trailing $p-1$ digits in n.

The upper bound p on the rank in the theorem is not always attained; for $p = 29$ the rank of $\{\nu_p(F_{n+1})\}_{n\ge0}$ is $15 = \alpha(29)+1$. However, it is attained for some values of p; for example, the rank is $11 = \alpha(11)+1$ for $p = 11$.

The proofs of the next two theorems mimic that of the previous theorem, so we omit the explicit matrices and some detail.

Theorem 2.2. *Let $p \equiv 13, 17 \mod 20$ be a prime such that $\nu_p(F_{\alpha(p)}) = 1$. Then $\{\nu_p(F_{n+1})\}_{n\ge0}$ is a p-regular sequence of rank at most $\frac{p+3}{2}$.*

Proof. We show that the $\frac{p+3}{2}$ sequences $\{\nu_p(F_{n+1})\}_{n\ge0}$ and $\{\nu_p(F_{pn+j+1})\}_{n\ge0}$ for $0 \le j \le \frac{p-1}{2}$ generate the $\mathbb{Z}$-module generated by the p-kernel of $\{\nu_p(F_{n+1})\}_{n\ge0}$.

In particular, we show for $n \geq 0$ that

$$\nu_p(F_{(pn+i)+1}) = \begin{cases} \nu_p(F_{pn+\left(i \bmod \frac{p+1}{2}\right)+1}) & \text{if } 0 \leq i \leq p-2 \\ \nu_p(F_{n+1}) + \nu_p(F_{pn+\frac{p-3}{2}+1}) & \text{if } i = p-1 \end{cases} \tag{2.12}$$

and that

$$\nu_p(F_{p(pn+i)+j+1}) = \nu_p(F_{pn+\left(i-j+\frac{p-3}{2} \bmod \frac{p+1}{2}\right)+1}) \tag{2.13}$$

for $0 \leq i \leq p-1$ and $0 \leq j \leq \frac{p-1}{2}$.

Vinson [7, Theorem 4] showed that if $p \equiv 13, 17 \mod 20$ then $4\alpha(p) = \pi(p)$. This allows us to refine Theorem 1.1 in this case and conclude that $\alpha(p)$ divides $(p+1)/2$.

Equation 2.12 is trivial for $0 \leq i \leq \frac{p-1}{2}$. For $\frac{p+1}{2} \leq i \leq p-2$, applying Theorem 1.2 and using that $1 \equiv -\frac{p-1}{2} \mod \alpha(p)$ shows that both sides are equal to

$$\begin{cases} \nu_p(F_{\alpha(p)}) & \text{if } \alpha(p) \mid pn+i+1 \\ 0 & \text{if } \alpha(p) \nmid pn+i+1. \end{cases}$$

For the case $i = p-1$ we apply Theorem 1.2 to all three valuations and see that both sides are equal to

$$\begin{cases} \nu_p(n+1)+2 & \text{if } \alpha(p) \mid n+1 \\ 0 & \text{if } \alpha(p) \nmid n+1 \end{cases}$$

under the assumption that $\nu_p(F_{\alpha(p)}) = 1$. We have used that $\alpha(p) \mid n+1$ precisely when $\alpha(p) \mid pn + \frac{p-1}{2}$, since $n+1 \equiv -\left(pn+\frac{p-1}{2}\right) \mod \alpha(p)$.

Theorem 1.2 shows that both sides of Equation 2.13 are equal to

$$\begin{cases} \nu_p(F_{\alpha(p)}) & \text{if } \alpha(p) \mid p(pn+i)+j+1 \\ 0 & \text{if } \alpha(p) \nmid p(pn+i)+j+1, \end{cases}$$

since $p(pn+i)+j+1 \equiv -\left(pn+\left(i-j+\frac{p-3}{2} \bmod \frac{p+1}{2}\right)+1\right) \mod \alpha(p)$. □

As in Theorem 2.1, the upper bound $(p+3)/2$ on the rank is not always attained. For example, for $p = 113$ the rank of $\{\nu_p(F_{n+1})\}_{n\geq 0}$ is $20 = \alpha(113)+1$ and for $p = 233$ the rank of $\{\nu_p(F_{n+1})\}_{n\geq 0}$ is $14 = \alpha(233)+1$.

The next theorem addresses the remaining classes of primes modulo 20, namely $p \equiv 3, 7 \mod 20$. However, we state it in the more general case for the residue classes $p \equiv 2, 3 \mod 5$, noting that Theorem 2.2 provides a better bound for $p \equiv 13, 17 \mod 20$.

Theorem 2.3. *Let $p \neq 2$ be a prime such that $p \equiv 2, 3 \mod 5$ and $\nu_p(F_{\alpha(p)}) = 1$. Then $\{\nu_p(F_{n+1})\}_{n\geq 0}$ is a p-regular sequence of rank at most $p+2$.*

Proof. We show that the $p+2$ sequences $\{\nu_p(F_{n+1})\}_{n\geq 0}$, $\{\nu_p(F_{p^2n+p+1})\}_{n\geq 0}$, and $\{\nu_p(F_{pn+j+1})\}_{n\geq 0}$ for $0 \leq j \leq p-1$ generate the $\mathbb{Z}$-module generated by the p-kernel of $\{\nu_p(F_{n+1})\}_{n\geq 0}$. In particular, we show for $n \geq 0$ that

$$\nu_p(F_{(pn+i)+1}) = \nu_p(F_{pn+i+1}) \tag{2.14}$$

for $0 \le i \le p-1$ (which is trivial), that

$$\nu_p(F_{p(pn+i)+j+1}) = \begin{cases} \nu_p(F_{pn+(i-j+p-1)+1}) & \text{if } i \le j-1 \\ -\nu_p(F_{n+1}) + \nu_p(F_{pn+(p-1)+1}) & \text{if } i = j \\ \nu_p(F_{p^2n+p+1}) & \text{if } i = j+1 \\ \nu_p(F_{pn+(i-j-2)+1}) & \text{if } i \ge j+2 \end{cases} \tag{2.15}$$

for $0 \le i \le p-1$ and $0 \le j \le p-2$ and

$$\nu_p(F_{p(pn+i)+(p-1)+1}) = \begin{cases} 2\nu_p(F_{pn+i+1}) & \text{if } 0 \le i \le p-2 \\ -\nu_p(F_{n+1}) + 2\nu_p(F_{pn+(p-1)+1}) & \text{if } i = p-1, \end{cases} \tag{2.16}$$

and that

$$\nu_p(F_{p^2(pn+i)+p+1}) = \begin{cases} \nu_p(F_{p^2n+p+1}) & \text{if } i = 0 \\ \nu_p(F_{pn+(i-1)+1}) & \text{if } 1 \le i \le p-1. \end{cases} \tag{2.17}$$

Note that $\alpha(p)$ divides $p+1$ by Theorem 1.1.

Theorem 1.2 establishes that for $i = j$ both sides of Equation 2.15 are equal to

$$\begin{cases} 1 & \text{if } \alpha(p) \mid n+1 \\ 0 & \text{if } \alpha(p) \nmid n+1; \end{cases}$$

for $i = j+1$ both sides are equal to

$$\begin{cases} 1 & \text{if } \alpha(p) \mid n \\ 0 & \text{if } \alpha(p) \nmid n; \end{cases}$$

and for the other two cases both sides are equal to

$$\begin{cases} 1 & \text{if } \alpha(p) \mid n-i+j+1 \\ 0 & \text{if } \alpha(p) \nmid n-i+j+1. \end{cases}$$

For $0 \le i \le p-2$, both sides of Equation 2.16 are equal to

$$\begin{cases} 2 & \text{if } \alpha(p) \mid n-i-1 \\ 0 & \text{if } \alpha(p) \nmid n-i-1 \end{cases}$$

under the assumption that $\nu_p(F_{\alpha(p)}) = 1$; for $i = p-1$ both sides are equal to

$$\begin{cases} 2 + \nu_p(n+1) + \nu_p(F_{\alpha(p)}) & \text{if } \alpha(p) \mid n+1 \\ 0 & \text{if } \alpha(p) \nmid n+1. \end{cases}$$

Finally, both sides of Equation 2.17 are equal to

$$\begin{cases} \nu_p(F_{\alpha(p)}) & \text{if } \alpha(p) \mid n-i \\ 0 & \text{if } \alpha(p) \nmid n-i. \end{cases} \qquad \square$$

As before, the upper bound $p+2$ on the rank is not always attained for $p \equiv 2, 3 \mod 5$. This is clear in view of the examples following Theorem 2.2. Additionally, there are examples of primes not congruent to 13 or 17 mod 20. For instance, for $p = 47$ the rank of $\{\nu_p(F_{n+1})\}_{n \ge 0}$ is $17 = \alpha(47) + 1$.

We conclude by showing that $\{\nu_p(F_{n+1})\}_{n \ge 0}$ is a p-regular sequence even when $\nu_p(F_{\alpha(p)}) \ne 1$.

Theorem 2.4. *Let p be a prime. Then $\{\nu_p(F_{n+1})\}_{n\geq 0}$ is a p-regular sequence.*

Proof. We assume $p \neq 2, 5$ because these cases are established by the comments at the beginning of the section.

Every periodic sequence is k-automatic for every $k \geq 2$ [2, Theorem 5.4.2]. Therefore the sequence whose nth term is

$$a(n) = \begin{cases} 1 & \text{if } \alpha(p) \mid n+1 \\ 0 & \text{if } \alpha(p) \nmid n+1 \end{cases}$$

is p-automatic and hence p-regular.

Let

$$b(n) = \begin{cases} \nu_p(n+1)+1 & \text{if } \alpha(p) \mid n+1 \\ 0 & \text{if } \alpha(p) \nmid n+1. \end{cases}$$

The previous theorems establish (without any condition on $\nu_p(F_{\alpha(p)})$) that the sequence $\{b(n)\}_{n\geq 0}$ is p-regular. Because p-regular sequences are closed under addition, it follows that $\{\nu_p(F_{n+1})\}_{n\geq 0} = \{b(n) + (\nu_p(F_{\alpha(p)}) - 1)a(n)\}_{n\geq 0}$ is p-regular. □

Note that if $\nu_p(F_{\alpha(p)}) \neq 1$ then the rank of $\{\nu_p(F_{n+1})\}_{n\geq 0}$ may be greater than the rank of $\{b(n)\}_{n\geq 0}$, so the upper bounds proved above for the rank of $\{b(n)\}_{n\geq 0}$ may not apply to $\{\nu_p(F_{n+1})\}_{n\geq 0}$. The following conjecture, based on extensive computer calculations, claims the exact value of the rank when $\nu_p(F_{\alpha(p)}) = 1$.

Conjecture. *Let $p \neq 2, 5$ be a prime such that $\nu_p(F_{\alpha(p)}) = 1$. Then the rank of the sequence $\{\nu_p(F_{n+1})\}_{n\geq 0}$ is $\alpha(p) + 1$.*

References

[1] Jean-Paul Allouche and Jeffrey Shallit, The ring of k-regular sequences, *Theoretical Computer Science* **98** (1992) 163–197; available at `http://www.cs.uwaterloo.ca/~shallit/Papers/as0.ps`.

[2] Jean-Paul Allouche and Jeffrey Shallit, *Automatic Sequences: Theory, Applications, Generalizations*, Cambridge University Press, Cambridge, 2003.

[3] J. D. Fulton and W. L. Morris, On arithmetical functions related to the Fibonacci numbers, *Acta Arithmetica* **16** (1969) 105–110; available at `http://matwbn.icm.edu.pl/ksiazki/aa/aa16/aa1621.pdf`.

[4] Tamás Lengyel, The order of the Fibonacci and Lucas numbers, *The Fibonacci Quarterly* **33** (1995) 234–239; available at `http://employees.oxy.edu/lengyel/papers/FQ/pdf/FnLn.pdf`.

[5] R. J. McIntosh and E. L. Roettger, A search for Fibonacci–Wieferich and Wolstenholme primes, *Math. Comp.* **76** (2007) 2087–2094.

[6] D. W. Robinson, The Fibonacci matrix modulo m, *The Fibonacci Quarterly* **1** (1963) 29–36.

[7] John Vinson, The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence, *The Fibonacci Quarterly* **1** (1963) 37–45.

[8] D. D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960) 525–532.

Department of Mathematics, Rutgers University, Piscataway, NJ 08854 and Department of Mathematics, University of Puerto Rico, San Juan, PR 00931

E-mail address: `lmedina@math.rutgers.edu`

Department of Mathematics, Tulane University, New Orleans, LA 70118

E-mail address: `erowland@tulane.edu`